12. Лемма Гаусса и следствие о содержании произведения многочленов.

Определение

Пусть $f(t) = a_n t^n + \dots + a_0 \in \mathbb{Z}[t]$. Тогда его содержание $c(f) = (a_0, \dots, a_n)$ (НОД коэффициентов).

Мы любим примеры:
Пусть $f(t) = 22t^2 + 4t + 2$ тогда $c(f) = (22,4,2) = 2$

Лемма 8

(Лемма Гаусса.) *Пусть $f, g \in \mathbb{Z}[x]$, $c(f) = c(g) = 1$. Тогда $c(fg) = 1$.*

Примерчик:
$f(t) = 2t^2 + 3t + 5$ и $c(f) = (2,3,5) = 1$
$g(t) = 1t^2 + 5t + 2$ и $c(g) = (1,5,2) = 1$

$fg(t) = 2t^4 + 13t^3 + 24t^2 + 31t + 10$ и $c(fg) = (2,13,24,31,10) = 1$

Доказательство. • Предположим противное и рассмотрим такое $p \in \mathbb{P}$, что $c(fg) \,\vdots\, p$. Однако, $c(f) \not\,\vdots\, p$ и $c(g) \not\,\vdots\, p$.

• Пусть $f(t) = a_n t^n + \dots + a_0$ и $g(t) = b_m t^m + \dots + b_0$. Рассмотрим такой наименьший индекс k, что $a_k \not\,\vdots\, p$ и такой наименьший индекс ℓ, что $b_\ell \not\,\vdots\, p$.

• Пусть $fg = d_{m+n} t^{n+m} + \dots + d_0$. Тогда

$$d_{k+\ell} = \left(\sum_{i=0}^{k-1} a_i b_{k+\ell-i} \right) + a_k b_\ell + \left(\sum_{i=k+1}^{k+\ell} a_i b_{k+\ell-i} \right) \not\,\vdots\, p,$$

так как первая сумма делится на p ($a_i \,\vdots\, p$ при $i \in \{0, \dots, k-1\}$) и вторая сумма делится на p (при $i \in \{k+1, \dots, k+\ell\}$ мы имеем $k + \ell - i \in \{0, \dots, \ell - 1\}$, а значит, $b_{k+\ell-i} \,\vdots\, p$), а $a_k b_\ell \not\,\vdots\, p$.

• Значит, $c(fg) \not\,\vdots\, p$, противоречие.

Чтобы понять о чем эта сумма посмотрим на нашем примере:
Пусть $k = 1$ и $l = 2$
$d_3 = a_0 \cdot b_3 + a_1 \cdot b_2 + a_2 \cdot b_1 + a_3 \cdot b_0 =$
$= 5 \cdot 0 + 3 \cdot 1 + 2 \cdot 5 + 0 \cdot 2 = 0 + 3 + 10 + 0 = 13$

Следствие 1

Для $f, g \in \mathbb{Z}[x]$ выполнено $c(fg) = c(f)c(g)$.

$f(t) = 22t^2 + 4t + 2$ и $c(f) = (22, 4, 2) = 2$
$g(t) = 3t^2 + 5t - 6$ и $c(g) = (3, 5, -6) = 1$

$fg(t) = 66t^4 + 122t^3 - 106t^2 - 14t - 12$ и
$c(fg) = (66, 122, -106, -14, -12) = 2$ $c(f)c(g) = 2 \cdot 1 = 2$

Доказательство. • Пусть $f(t) = c(f) \cdot f_1(t)$ и $g(t) = c(g) \cdot g_1(t)$.

• Тогда $f_1, g_1 \in \mathbb{Z}[t]$ и $c(f_1) = c(g_1) = 1$ и по Лемме Гаусса $c(f_1 g_1) = 1$.

• Следовательно,

Эта штучка равна 1

$c(fg) = c(c(f) \cdot f_1 \cdot c(g) \cdot g_1) = c(f)c(g) \cdot c(f_1 g_1) = c(f)c(g)$ (мы воспользовались тем, что общий множитель $c(f)c(g)$ при вычисления НОД коэффициентов можно вынести). $\square$

Например, $f_1(t) = 11t^2 + 2t + 1$

$fg(t) = 66t^4 + 122t^3 - 106t^2 - 14t - 12$ и
$c(fg) = c(\,2 \cdot (11t^2 + 2t + 1) \cdot 1 \cdot (3t^2 + 5t - 6)) = 2 \cdot 1 \cdot c(f_1 g_1) =$
$= 2 \cdot 1 \cdot 1 = 2$

13. Лемма о связи разложений многочлена с целыми коэффициентами на множители в Q[x] и в Z[x]. Эквивалентность неприводимости в Z[x] и в Q[x].

Лемма 9

Пусть $f \in \mathbb{Z}[x]$, $q_1, \dots, q_n \in \mathbb{Q}[x]$, $f = q_1 \dots q_n$, $\deg(q_i) \geq 1$ для всех $i \in \{1, \dots, n\}$. Тогда существуют такие $p_1, \dots, p_n \in \mathbb{Z}[x]$ и $c_1, \dots, c_n \in \mathbb{Q}$, что $f = p_1 \dots p_n$ и $p_i = c_i q_i$ для всех $i \in \{1, \dots, n\}$.

Эта теорема о том, что мы можем разложить каждый многочлен на произведение нескольких других как с целыми, так и рациональными коэффициентами.

$$f(t) = a_2 t^2 + a_1 t + a_0 = (q_{0,1} t + q_{0,0})(q_{1,1} t + q_{1,0})(q_{2,1} t + q_{2,0}) =$$

$$= (p_{0,1} t + p_{0,0})(p_{1,1} t + p_{1,0})(p_{2,1} t + p_{2,0})$$

Доказательство. • Для каждого $i \in \{1, \dots, n\}$ представим все коэффициенты q_i в виде несократимых дробей, пусть m_i — НОК знаменателей этих коэффициентов. У каждой такой скобки будет свой m

• Тогда $g_i = m_i q_i \in \mathbb{Z}[x]$ и $mf = g_1 \dots g_n$, где $m = m_1 \dots m_n \in \mathbb{N}$.

$$f(t) = m_0(q_{0,1} t + q_{0,0}) \cdot m_1(q_{1,1} t + q_{1,0}) \cdot m_2(q_{2,1} t + q_{2,0}) =$$

$$= m \cdot (q_{0,1} t + q_{0,0})(q_{1,1} t + q_{1,0})(q_{2,1} t + q_{2,0})$$

Утверждение

Пусть $mf = g_1 \dots g_n$, где $m \in \mathbb{N}$, $f, g_1, \dots, g_n \in \mathbb{Z}[x]$. Тогда существует разложение $f = p_1 \dots p_n$, где $p_i = d_i g_i \in \mathbb{Z}[x]$, $d_i \in \mathbb{Q}$ для всех $i \in \{1, \dots, n\}$.

Доказательство. Индукция по m.

База $m = 1$: построенное разложение $f = g_1 \dots g_n$ подходит.

Переход. • Пусть для меньших m утверждение доказано, $p \in \mathbb{P}$, $m \,\vdots\, p$.

• Тогда $c(g_1) \dots c(g_n) = c(g_1 \dots g_n) = c(m \cdot f) \,\vdots\, p$, значит, существует такое $i \in \{1, \dots, n\}$, что $c(g_i) \,\vdots\, p$.

• НУО $c(g_1) \vdots p$. Тогда $g_1 = p \cdot g_1^*$, где $g_1^* \in \mathbb{Z}[x]$.

• Пусть $m^* := \frac{m}{p}$. Тогда $m^* \in \mathbb{Z}$ и $m^* f = g_1^* g_2 \dots g_n$.

• Так как $m^* < m$, по индукционному предположению существует разложение $f = p_1 \dots p_n$, где $p_1 = d_1^* g_1^*$ и $p_i = d_i g_i$ при $i \in \{2, \dots, n\}$.

• Положим $d_1 := \frac{d_1^*}{p}$. Тогда $p_1 = d_1 g_1$, получено разложение для m. $\square$

• Для завершения доказательства леммы остается положить $c_i := d_i m_i$. $\square$

• Если многочлен $f \in \mathbb{Z}[x]$ неприводим в $\mathbb{Q}[x]$, то он, очевидно, неприводим и в $\mathbb{Z}[x]$.

Следствие 2

Многочлен $f \in \mathbb{Z}[x]$ неприводим в $\mathbb{Q}[x]$, если и только если он неприводим в $\mathbb{Z}[x]$.

Доказательство. $\Rightarrow$. Если многочлен $f \in \mathbb{Z}[x]$ приводим в $\mathbb{Z}[x]$, то он, очевидно, приводим и в $\mathbb{Q}[x]$.

$\Leftarrow$. • Предположим противное, пусть f приводим в $\mathbb{Q}[x]$.

• Тогда $f = g_1 g_2$, где $g_1, g_2 \in \mathbb{Q}[x]$, $1 \le \deg(g_1) < \deg(f)$ и $1 \le \deg(g_2) < \deg(f)$.

• По Лемме 9, существует разложение $f = h_1 h_2$, где $h_1, h_2 \in \mathbb{Z}[x]$, $h_1 = c g_1$ и $h_2 = c' g_2$, $c, c' \in \mathbb{Q}$.

• Тогда f приводим в $\mathbb{Z}[x]$, противоречие. $\square$

16. Свойства рациональных корней и значений в целых точках многочленов с целыми коэффициентами.

Лемма 10

Пусть $f(t) = a_n t^n + \dots + a_0 \in \mathbb{Z}[t]$, $x, y \in \mathbb{Z}$, $x \neq y$. *Тогда* $f(x) - f(y) \,\vdots\, x - y$.

Доказательство. • НУО $x - y > 0$. Так как $x \equiv_{x-y} y$, для всех $k \in \{0, \dots, n\}$ выполняется $x^k \equiv_{x-y} y^k$.

• Тогда $f(x) = \sum\limits_{k=0}^{n} a_k x^k \equiv_{x-y} \sum\limits_{k=0}^{n} a_k y^k = f(y)$. □

Лемма 11

Пусть $f(t) = a_n t^n + \dots + a_0 \in \mathbb{Z}[t]$, $f(\frac{p}{q}) = 0$, *где* $p, q \in \mathbb{Z}$, $(p, q) = 1$. *Тогда* $a_n \,\vdots\, q$ *и* $a_0 \,\vdots\, p$.

Доказательство.

$$0 = q^n f(\tfrac{p}{q}) = a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n. \qquad (1)$$

• Все слагаемые в правой части (1), кроме $a_n p^n$, делятся на q, значит, и $a_n p^n \,\vdots\, q$. Так как $(p, q) = 1$, получаем $a_n \,\vdots\, q$.

• Все слагаемые в правой части (1), кроме $a_0 q^n$, делятся на p, значит, и $a_0 q^n \,\vdots\, p$. Так как $(p, q) = 1$, получаем $a_0 \,\vdots\, p$. □

Следствие 4

Пусть $f(t) = t^n + \dots + a_0 \in \mathbb{Z}[t]$, $\alpha \in \mathbb{Q}$, $f(\alpha) = 0$. *Тогда* $\alpha \in \mathbb{Z}$.

Доказательство. • Пусть $\alpha = \frac{p}{q}$, где $p, q \in \mathbb{Z}$, $(p, q) = 1$.

• По Лемме 11, $1 \,\vdots\, q$, то есть $\alpha \in \mathbb{Z}$. □

Лемма 12

Пусть $f(t) = a_n t^n + \dots + a_0 \in \mathbb{Z}[t]$, $f(\frac{p}{q}) = 0$, *где* $p, q \in \mathbb{Z}$, $(p, q) = 1$. *Тогда* $f(k) \vdots kq - p$ *для любого* $k \in \mathbb{Z}$.

Доказательство. •

$$q^n f(k) = q^n\left(f(k) - f\left(\frac{p}{q}\right)\right) = \text{Раскрыли скобки и записали в виде суммы}$$

$$\left(\sum_{i=0}^{n} q^n a_i k^i\right) - \left(\sum_{i=0}^{n} a_i p^i q^{n-i}\right) = \sum_{i=1}^{n} q^{n-i} a_i\left((kq)^i - p^i\right) \vdots kq - p,$$

так для всех $i \in \{1, \dots, n\}$

$(kq)^i - p^i \vdots kq - p \iff (kq)^i \equiv_{kq-p} p^i \Leftarrow kq \equiv_{kq-p} p$.

• Так как $(q^n, kq - p) = (q, p) = 1$, из $q^n f(k) \vdots kq - p$ следует, что $f(k) \vdots kq - p$.

□

17. Разностный многочлен.

Определение

Пусть $f \in K[x]$, где K — коммутативное кольцо с 1, причем $K \supset \mathbb{Z}$.

• Разностный многочлен задается формулой $\Delta f(x) := f(x+1) - f(x)$.

• Примеры подходящих колец K: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Пусть $f(x) = 2x^2 + 3x + 5$ и тогда $f(x+1) = 2(x+1)^2 + 3(x+1) + 5$

$$\Delta f(x) = 2x^2 + 4x + 2 + 3x + 3 + 5 - (2x^2 + 3x + 5) = 4x + 5$$

Лемма 13

Пусть $f \in K[x]$, где K — коммутативное кольцо с 1, причем $K \supset \mathbb{Z}$. Тогда $\Delta f \in K[x]$, $\deg(\Delta f) = \deg(f) - 1$.

Доказательство. • Пусть $f(x) = a_n x^n + \dots + a_0$, где $n = \deg(f)$.

Давайте рассмотрим какие-то два слагаемых разницы из многочленов

• По биному Ньютона, $a_k\big((x+1)^k - x^k\big) = \sum\limits_{i=1}^{k} a_k \mathrm{C}_k^i x^{k-i}$.

• Поэтому $\Delta f \in K[x]$.

• Одночлены с x^n в Δf сокращаются, а единственный одночлен с x^{n-1} — это $a_n \mathrm{C}_n^1 x^{n-1}$ с коэффициентом $a_n \mathrm{C}_n^1 \neq 0$. Следовательно, $\deg(\Delta f) = n - 1$. □